SUCCESS STORY

➢ High Integrity Systems ➢

Abstract Interpretation Saves $1 Million, 1 Year in Verifying Fault Tolerant Controller

The new Abstract Interpretation method has saved $1 million and up to one calendar year in verifying fault tolerant controller software used in critical process manufacturing applications that require a high degree of reliability and availability. Triconex's Trident systems provide continuous control for safety-critical units in refineries, petrochemical and chemical plants and other industrial processes. In previous versions of the system, up to five-man years were needed to perform white-box testing to ensure the absence of runtime errors. For the latest release, Gershon Shamay, Software Development Manager for the Irvine, California based division of Invensys, decided to try the Abstract Interpretation method, which automatically checks the dynamic properties of software applications without actually running any test case and without executing it. "We spent a day setting up the software and then let it run on a high-end PC," Gershon said. "The tool provided exhaustive coverage of every possible combination of input variables and generated a report of every possible runtime error. We saved about 10,000 man-hours of testing and released our product between six and twelve months earlier than would have otherwise been possible."

Triconex's Trident provides continuous protection for safety critical units while avoiding the dangerous nuisance trips that often occur with traditional shutdown systems implemented with mechanical or electronic relays. The state-of-the-art controller provides fault tolerance by means of a triple modular redundant architecture that integrates three isolated, parallel, control systems and extensive diagnostics. The three independent systems execute the application program in parallel. The system uses two-out-of-three voting to provide high-integrity, error-free, uninterrupted process operation with no single point of failure. If a hardware failure occurs in one channel, the other channels override it and the faulty channel can be replaced while the controller is online without interrupting the process. In a typical application, signals that determine whether a plant is operating safely – such as pressure, temperature and product feed rates – are monitored and shutdown actions taken if an upset condition occurs. In addition to a TUV certification for DIN AK levels 1 through 6, additional product certification and verification includes IEC 61508 – SIL3, CSA/NRTLC/C, European Union CE Mark, and Factory Mutual Class I, Division 2 Temperature T4, Groups A, B, C and D.

White-box testing is critical

The burden of developing a product that performs such a safety-critical task is that every new version must pass exhaustive testing before it is released. The company's newest 1.2 version adds support for two new types of IO modules and one new communications module. In addition, the internal dynamics of the system have been changed to make it faster and more responsive. Of course, the product must pass the functional or black box testing required of nearly every software product to ensure that it operates correctly from the user's standpoint. In addition, because of the critical nature of this application, Triconex's quality staff and the product testing agencies that certify its products also require that it pass white box testing designed to provide objective evidence that the software is truly error free.

This is a very challenging task for a system that has on the order of 70,000 lines of C, 140,000 lines of Ada and operates in triplicate in hard real time so it can shut down a plant within milliseconds if specified safety boundaries are exceeded. The challenge was detecting runtime errors e.g. processor halt, data corruption, timing violations, etc. Such runtime errors can also cause applications to send erroneous commands to external devices, causing costly nuisance shutdowns. In the past, the company handled the job manually, relying upon intensive multilevel and system testing by experienced quality engineers who developed test scripts and procedures designed to weed out errors. A complete 'white box' test of such a product can easily consume 4 to 5 man-years of effort, spread over 6 to 12 calendar months in order to satisfy the quality staff and obtain certification from government agencies.

invensys

PolySpace TECHNOLOGIES

The alternative Abstract Interpretation

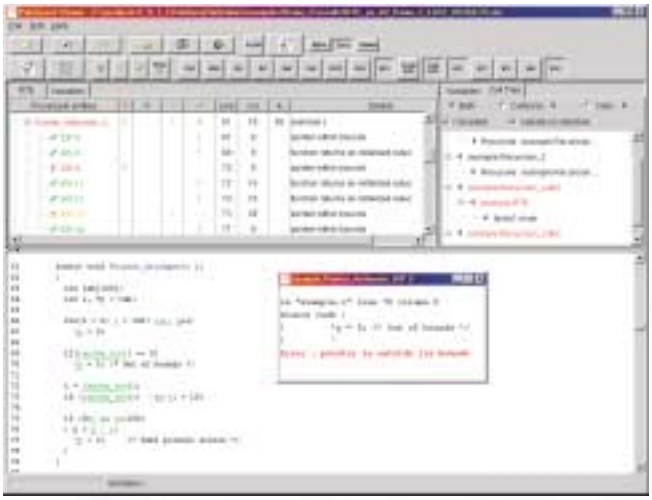
Gershon has been seeking an alternative for a considerable period of time. While reducing testing costs and bringing products to market sooner was of interest, his main concern was obtaining assurance that the company had actually tested every possible input permutation. Triconex already makes intensive use of automated testing tools that detect errors that occur in defined cases but provide less than exhaustive coverage of the application. The amount of computational time required to evaluate every case of even a small application using these tools would be prohibitive. About a year ago, Gershon attended an embedded systems conference looking for tools that would assist in the verification process. He visited the vendors that exhibited at the show and asked for a demonstration of how their tools work. He found a variety of different approaches but the one that appeared most suited to his needs were the C Verifier and Ada Verifier tools from Polyspace, Beverly, Massachusetts, which have pioneered a new technology called Abstract Interpretation.

Instead of iteratively verifying software states like a case generator, the Polyspace tools work on an abstraction of the analyzed software built from its dynamic properties. For example, if a variable is designed to accept integers between 1 and 1000 (loop index), a case generator would require that the code be executed 1000 times in conjunction with every possible combination of the other input variables. This is an enormous computational task and helps demonstrate why case test generators are incapable of exhaustive testing. The Abstract Interpretation model used by PolySpace Verifier, on the other hand, only evaluates the code a single time from its dynamic properties, greatly reducing the computational load. In the example above, the variable is reduced to a discrete data increasing from 1 to 1000. The obvious advantage of the new approach to software verification is that it can automatically check 100% of runtime errors in a tiny fraction of the time that would be required to exhaustively test the code using traditional verification methods. The software is now used to test critical systems by companies such as EADS, Honeywell, Snecma, NASA, Smiths Industries, GE, Alcatel Space, BAe Systems, Alstom, CSEE Transport, Nissan, NTT DoCoMo, France Telecom, and many others.

Exhaustive verification in minimal time

“I asked them to provide their software to test our new release,” Gershon said. “They sent out a person who installed PolySpace C Verifier and Ada Verifier on a Linux PC they brought. They copied my source code to the new system and within a day they were ready to start the test procedure. The tool analyzed eight software subsystems at an average elapsed time of less than a day each. When the test was done, it generated a 20-page document containing attempts to read non-initialized variables, access conflicts for unprotected shared data, referencing through null or out-of-bounds pointers, etc. We then analyzed each of the conditions highlighted in the report based on our knowledge of the system. We determined that several of the conditions that were highlighted in the report were not really errors but rather caused by the fact that the dynamics of a system in which three copies are running simultaneously limited the visibility of the testing tool. Within a week after the test was completed, we had covered every item identified in the report and determined that the software was ready to release.”

Gershon said that in the end Triconex saved four to five man-years of time that allowed the company to bring its product to market somewhere between six to twelve months earlier than would have been possible using its previous methods. “But in my opinion the most important improvement is that we are now certain that we have examined every line of code under every possible input condition,” he said. “The certification agencies agree with this assessment. They have encouraged us in the past to move to full visibility verification methods and they certified our newest product in record time based on the PolySpace reports. As a result, we will use now PolySpace to provide full-visibility verification of all new releases of all our products. We are already using the tool in a new computer-based interlocking application product that is being developed in partnership with Invensys Rail Systems to help move trains to their intended destination while preventing collisions.”



PolySpace TECHNOLOGIES

Email: contact-usa@polyspace.com
www.polyspace.com